University of Bahrain
IT College, CS Department

ITCS 412: Cryptography
First Semester 2013/2014
Test II

St. ID :
Name : DRAGON
Section :

9:00 | 12:00

This exam consists of **5** pages. Duration: One hour

	Part 1	Part2	Part 3	Total
Maximum	10	20	10	40
Grade	6	18	9	33

Part 1:

Answer the following questions by clearly circling the *most appropriate* answer [1 point each]

1. In the case of the digital signature, the hash value of a message is encrypted with a user's private key. Anyone who knows the user's public key can verify the integrity of the message. Is this statement true or false?
   a. True
   b. False

2. In hash function requirements, for any given hash value *h*, it is computationally feasible to find *y* such that H(*y*)= *h*. Is this statement true or false?
   a. True
   b. False

3. Which of the following is **not** a requirement for a hash function H,
   a. H produces a variable length output
   b. It is computationally infeasible to find any pair (x,y) such that H(x) = H(y).
   c. For any x it is computationally infeasible to find y≠x such that H(y)=H(x).
   d. For any h it is computationally infeasible to find x such that H(x)=h.

4. Which of the following techniques is the best for the distribution of public keys:
   a. Public announcement
   b. Publicly available directory
   c. Public-key certificates
   d. Public Authority
   e. All of the above

5. Which of the following is <u>not</u> a many-to-one function for message *M*

   a. MAC (*M*, *K*)
   b. Hash (*M*)
   c. RSA_Encryption (*M*, *e*, *n*) , where *e* and *n* are the public key
   d. Digital Signature (*M*)

6. Which of the following is ***not*** true on a Certificate scheme:

   a. Only the CA can create and update certificates.
   b. Only the participant can sign certificates
   c. Any participant can read a certificate
   d. Any participant can verify that the certificate originated from the certificate authority (CA).

7. Message Authentication is concerned with:

   a. Protecting e-Commerce applications
   b. Protecting the integrity of a message
   c. Provide the identity of an attacker
   d. Provide authentication and confidentiality

8. In simple key distribution, Man-in-the-Middle Attack can occur by opponent who may impersonate both communicating parties ***A*** and ***B*** as follows:

   1. A generates $[PU_A, PR_A]$ and transmits (PU_A, ID_A) to B
   2.
   3. B generates secret key K_s and sends $E(K_s, PU_E)$ to A
   4. E intercepts, learns K_s from $D(E(K_s, PU_E), PR_E)$
   5. E transmits $E(K_s, PU_A)$ to A

   Step no. 2 is missing, which of the following is the missing step:

   a. E intercepts, creates $[PU_E, PR_E]$, sends (PU_E, ID_A) to A
   b. E intercepts, creates $[PU_E, PR_E]$, sends (PU_E, ID_E) to B
   c. E intercepts, creates $[PU_E, PR_E]$, sends (PU_E, ID_A) to B
   d. E intercepts, creates $[PU_E, PR_E]$, sends (PR_E, ID_A) to B

9. On many occasions, systems have been broken not because of a poor encryption algorithm, but because of poor key selection or management. Which of the following is a desirable action to the above matter

   a. frequent key changes
   b. frequent algorithm changes
   c. Use multiple encryption algorithms
   d. Use multiple key-exchange algorithms

10. Which of the following is an SSL protocol?

    a. Handshake protocol
    b. Transport layer security protocol
    c. RSA key-exchange protocol
    d. Connection and session authentication protocol

Part 2:

1. Suppose that Alice chooses for an RSA system the primes $p = 29$, and $q = 17$, and the public key $e = 31$. [4 points]

   (a) Write the equation to encrypt the plaintext $M = 245$.

   $n = p.q$

   $C = M^e \bmod n$ $\Rightarrow$ $C = 245^{31} \bmod (29 \times 17)$

   (b) Write the equation to determine the private key d.

   $\phi(n) = (p-1)(q-1)$
   $= (28 \times 16)$ $\Rightarrow$ $e.d = \phi(n) + 1$, $d = \frac{(28 \times 16)+1}{31}$

   4

2. In the RSA public encryption scheme:

   i. What are the steps for RSA key generation i.e. creating the public and private key.

   The first and last steps are given for you. [3 points]

   1. Selecting two large primes at random : p, q
   2. find $n = p.q$ and $\phi(n) = (p-1)(q-1)$
   3. find e such that $\gcd(e, \phi(n)) = 1$
   4. find $e.d \bmod \phi(n) = 1$
   5. publish the public encryption key: KU={e,N}
   6. keep secret private decryption key: KR={d,N}

   3

3. Given a hash value h with a n-bit length for an unknown message m. Explain a brute force attack to find a message with the same hash value h and the level of effort. [2 points]

   2

   try all possible messages with n-bit and hash them to find matching hash. it will take on average $\frac{2^n}{2}$.

4. Explain an attack by an adversary whom wishes to find two messages or data blocks, x and y, that yield the same hash function: H(x) = H(y). [3 points]

   using birthday attack. in birthday attack, 2 in 23 people have probibality > 0.5 to share the birthday. So an adversary will generate two messages and then hash them to find a match

   2

   it will take him about $2^{m/2}$ on average. becaus of the birthday attack.

5. List two main functionalities that digital signatures provide [2 points]

2
i. authenticate message content.
ii. verify the identity of sender.

6. To provide both confidentiality and authentication to a message *M*, A can encrypt *M* first using its private key, which provides the digital signature, and then using B's public key, which provides confidentiality. What is the disadvantage of this approach? [1 point]

1
it will require two encryption and decryption, which will be very slow using public-key encryption.

7. Assume two communicating parties A and B authenticated each other. Now A and B want to communicate messages and authenticate them without the burden of using public key. What do you propose? [2 points]

1
they can use certificate authority or use a session key for this session.
how

8. Explain why MAC is not a digital signature. [1 points]

1
because both sender and receiver know the key.

9. A brute force attack on hash function depends solely on the length of hash code. A brute force attack on MAC depends on two factors? [2 points]

2
it depends on the length of the MAC and the key that used to generate it.

Part 3:

1. What protocols comprise SSL? [2 points]

2
i. SSL record protocol
ii. SSL change cipher spec protocol
iii. SSL handshake protocol
iv. SSL alert protocol.

2. What is SSL Session. [1 points]

1
it is a communication link between client and server. SSL session can have multiple SSL connection.

3. What is the purpose of the dual signature in SET protocol? [2 points]

2
the purpose is to verify the order information and payment information. because a merchant should know only the order information, and the bank should only know the payment information.

4. In SET protocol, the merchant forwards to the payment Gateway (bank) encrypted blocks of related payment information sent by the cardholder. What do the encrypted blocks contain? and what type of verification the payment gateway performs from it?

[3 points]

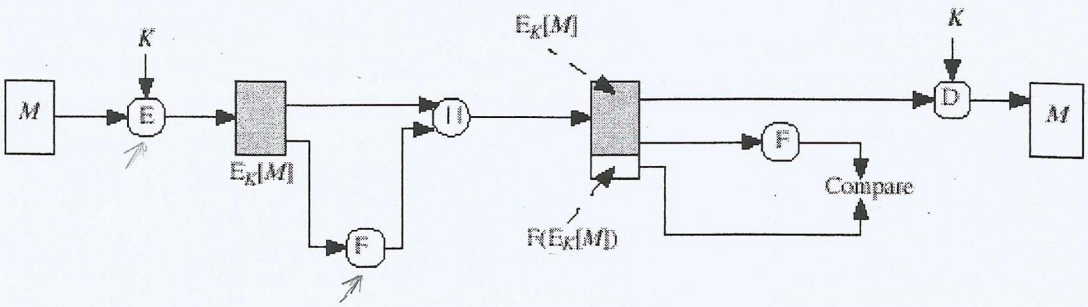
the encrypted blocks contain the payment information, the hash value of the order information, and the dual signature.

the verification is to check if the payment information is linked to the order information or not.

3

5. In the figure below, the order in which hash and encryption functions are performed is critical. What may go wrong with the below scheme? (F is a hash function).

[2 points]



the problem in this scheme is that the encryption happen before the hash. So the messages hash depends on the encrypted message not the message itself. So if somthing goes wrong in the encryption it will result problems.

1